Analysis of electronic and telematic voting systems in binding experiences

Emilia Pérez Belleboni, Justo Carracedo Gallardo, Ana Gómez Oliva, Sergio Sánchez García

ABSTRACT

This paper is about analysis and assess of three experiences on telematic and electronic voting dealing with such aspects as security and achievement of the social requirements. These experiences have been chosen taking into account the deepness of the public documentation and the technological challenge they faces.

Keywords

Electronic & telematic voting systems

1. INTRODUCCIÓN

En distintos países, entre los que cabe destacar, dentro del área iberoamericana, Brasil y Venezuela, se han implantado, con bastante éxito, sistemas de *voto electrónico* consistentes en la de automatización de la emisión del voto y la realización de escrutinios desde sitios especialmente habilitados para ello, como sucede en la votación tradicional. Mientras en Europa se asentando la posibilidad de realizar la votación desde ordenadores particulares conectados a Internet, tomando ciertas medidas de seguridad en los procesos telemáticos. Estonia, por su perseverancia en llevar adelante el proyecto de estas características, y Noruega por lo novedoso, marcan hitos en la evolución del voto electrónico hacia el voto telemático.

2. EXPERIENCIAS

Según la información oficial ofrecida por (1), la República Federal de Brasil tiene una extensión de 8.514.876,60 km^2 y 190.732.694 habitantes, de los cuales unos 135 millones tuvieron derecho a voto en las elecciones presidenciales de ese año. Desde hace más de una década despliega dispositivos de votación electrónica que permitan con más garantía que con los procesos manuales, recabar la voluntad de todos los ciudadanos.

La República de Estonia (2), de 45.000 km^2 y cerca de 1.300.000 habitantes tiene el mérito de ser el primer país que incorpora oficialmente, en votaciones vinculantes, la posibilidad de que sus ciudadanos entreguen los votos vía Internet. Este sistema de votación está incluido en un plan de modernización del país que, desde el año 2000, abarca el despliegue del documento de identidad electrónico y posibilidades de comunicación entre los ciudadanos y la Administración en una gran variedad de trámites.

Noruega (3) 385.252km^2 con unos 5.000.000 de habitantes Noruega ha aplicado en septiembre de 2011 un sistema pionero de voto por Internet combinado con su sistema de identificación electrónica que no usa tarjeta inteligente.

2.1 Brasil

En Brasil, las mesas electorales están a cargo de representantes nombrados por los partidos políticos y de voluntarios que se ofrecen ante los tribunales regionales electorales. En este país es voluntario el ejercicio del voto para quienes estén en la franja entre 16 y 18 años y los mayores de 70, y obligatorio para los que se encuentran entre 18 y 70 años, bajo penalización de pérdida de derechos tan fundamentales como la obtención de pasaporte o documento de identidad (4), entre otras sanciones. El portal oficial del Gobierno de Brasil (5), en su apartado dedicado a la historia de las votaciones, indica que en 1994 se empezó el proceso de recepción de votos en urnas electrónicas, en principio para una parte de los votantes del país, y que en el año 2000 este procedimiento estuvo al alcance de la totalidad de los votantes. La introducción de la urna electrónica tiene su fundamento en interminables acusaciones de fraude electoral en la historia del país. Las urnas que se han aplicado han evolucionado con el tiempo, desde las que usaron el sistema operativo propietario tipo Windows, al uso de Software Libre Linux. Algunas de las urnas usadas han sido fabricadas por Diebold (6) y por UNiSYS (7), empresas que han recibido fuertes críticas en diversos foros (8), (9). La tendencia actual consiste en la incorporación de urnas capaces de emplear información biométrica (fotografía y huellas dactilares) para la identificación de votantes como paso previo para depositar el voto. Bajo el título de "información técnica", el Tribunal Superior Electoral de Brasil ofrece información (10) sobre los procedimientos conducentes a ganar la confianza de electores y participantes en la contienda electoral, estableciendo los plazos y lugares en los que se llevan a cabo auditorías de distintas partes del proceso, haciendo hincapié en el uso de la firma electrónica del software y la generación de resumen (*hash*) para permitir la verificación de la autenticidad del software en diversas etapas del procedimiento. En este portal, cualquier internauta puede ver, desde el punto de vista del votante, el funcionamiento del simulador oficial del sistema de votación. De especial interés para tener la visión oficial del sistema resultan los documentos creados para servir de guía a los miembros de la mesa electoral. Brasil tiene en marcha el proyecto de despliegue del *Registro de Identidade Civil*, RIC (documento de identidad electrónico) (11), mediante el cual se tiene la intención de formar un censo con registro biométrico, incluyendo foto y las 10 huella dactilar las manos, que llegue a toda su población antes de 2019. Aunque ya accedieron mediante identificación biométrica a las elecciones presidenciales de 2010 alrededor de 1 millón de electores.

2.1.1 *Urna Electrónica y Urna Biométrica*

El sistema electoral brasileño tiene una parte de trabajo manual y otra parte automatizada. La parte manual incluye, entre otras, las tareas realizadas por los miembros de la mesa electoral: la identificación de votantes, emisión de justificantes y firma de las actas. Básicamente, cuando se habla de Urna Electrónica, se quiere decir que está automatizada la tarea correspondiente a la emisión del voto, al recuento de los mismos así como la generación de actas en papel y en algún dispositivo de almacenamiento magnético. El elector, tras presentar su identificación en la puerta, se presenta e identifica nuevamente ante los miembros de la mesa. Estos lo buscan en las listas y, desde el terminal de la mesa, autorizan al elector a emitir un voto desde el terminal de votante. Finalmente los miembros de la mesa toman nota del evento finalizado. Los miembros de la mesa deben controlar que la persona que accede al terminal de votante es la misma persona que se ha identificado. Las actas se envían en soporte físico hacia los centros oficiales del Tribunal Superior Electoral, aunque en la actualidad algunos sitios experimentan la comunicación de los resultados vía satélite (12). También es tarea de los miembros de la mesa electoral realizar la instalación de los terminales de votante y de la mesa, que interconectados, permiten el proceso. Es de destacar que estos dispositivos se reciben lacrados para prevenir la manipulación en su interior y no se conectan a ninguna red de transmisión de datos.

Aunque han disminuido las acusaciones de fraude electoral, en distintos foros se pone de manifiesto la preocupación por la robustez del censo de electores y la verificación de que la persona que vota es la misma que se ha identificado. Con el objetivo de abordar esta realidad, últimamente se ha incorporado la identificación biométrica de los electores para impedir la suplantación de los mismos. La gran diferencia entre las urnas electrónica biométrica es que la última tiene el registro de huella dactilar de todos los votantes. Así la huella capturada en el terminal de la mesa es comparada con el registro y si coincide se habilita automáticamente el terminal de para recibir el voto. Siguen siendo los miembros de la mesa responsables de controlar que la persona que accede al terminal de votante es la misma persona que se ha identificado. Debido a la incidencia de posibles errores en la identificación biométrica de votantes, desde el terminal de la mesa se puede habilitar manualmente el terminal de votación, registrando en un cuaderno la ocurrencia de este evento.

2.1.2 *Valoración*

La sustitución del método tradicional de urna como contenedor físico de los votos en papel tiene detractores que ven en este nuevo sistema nuevas formas de realizar fraude electoral. Además de presentar dudas sobre las características de la tecnología utilizada, las faltas de disciplina en el cumplimiento de los procedimientos y la ausencia de respuestas a las denuncias presentadas son objeto de análisis (13). Una de las críticas técnicas de una gravedad indiscutible es que la identificación biométrica se realice en una máquina que está conectada con la que recibe el voto, lo cual puede abrir una vía para establecer la relación entre voto y votante. Para solucionar in-situ el problema de la identificación biométrica que es susceptible de producir "falsos negativos", los miembros de la mesa electoral tienen la capacidad de desbloquear el terminal de votante y permitir el voto. L adición de votos ilegítimos por acuerdo de los miembros de la mesa de no reflejar la incidencia en el cuaderno apropiado, no es un riesgo inherente al voto electrónico, ya que está presente también en el voto tradicional.

A continuación se exponen diversas posibilidades de actuación que pueden dar como resultado la alteración fraudulenta o accidental de resultados de una votación, aplicando este sistema:

2.1.2.1 *Posibilidad de inclusión de votos ilegítimos*

Tanto en el caso de urna electrónica como en el caso de urna biométrica, desde el terminal de la mesa se puede habilitar el terminal de votación, acompañado del registro manual del evento en el cuaderno de votación. En caso de colusión entre los miembros de la mesa, la inclusión de votos en nombre de los que no han asistido es una probabilidad real. Cuando la identificación es biométrica, el votante en nombre del cual se incluyó el voto, será llamado a renovar su registro biométrico, con lo cual puede sospechar lo que ha ocurrido, pero por otra parte, con este acto ilícito los miembros de la mesa han salvado al ciudadano de una sanción que le acarrearía graves trastornos, por lo que no sería extraño que no intentara evidenciar el fraude. La ausencia del votante en la jornada electoral se puede deber a una amplia variedad de motivos, entre las cuales no se puede dejar de considerar, por su gravedad, la "compra de abstenciones" con objeto de realizar el fraude antes comentado que no es inherente ni exclusivo del proceso electrónico.

2.1.2.2 *Posibilidad de modificación de votos*

Se puede modificar o eliminar votos manipulando el software de los terminales de forma que dicha alteración no fuera detectada por la auditoría. En el manual para los miembros de la mesa (14), no se les atribuye la tarea de realizar la verificación del software, el cual se supone está firmado. De aquí se puede deducir que la última auditoría se ha hecho en un paso previo, en el cual se ha procedido a poner el lacrado al hardware. Es decir esta posibilidad se puede materializar en caso de auditoría o lacrado inadecuado.

2.1.2.3 *Denegación arbitraria del derecho de voto*

La composición de la mesa electoral con representación de los candidatos ofrece las garantías de que la denegación arbitraria de este derecho sería denunciada, salvo que se debiera a una manipulación del censo electoral. Este riesgo, como los anteriores no es consecuencia de la aplicación de sistemas electrónicos.

2.1.2.4 *Coacción de votantes*

La posibilidad más clara de coacción de votantes es la encaminada a asegurarse su abstención con objeto de usarla aprovechando las características de la propia mecánica de votación. Otra posibilidad se puede materializar actuando sobre el censo, si bien estos métodos no corresponden a un fraude específico de un sistema de voto electrónico.

2.1.2.5 *Posibilidad de ruptura del secreto del voto*

Debería aportarse exhaustiva información que permita ofrecer garantías totales de que: No habrá posibilidad de establecer la relación votante-voto haciendo un seguimiento del registro de votantes en la misma secuencia temporal en la que se han emitido los votos y que la identificación biométrica realizada en un sistema conectado al terminal en el que se emite el voto no es utilizada para conocer el voto del votante.

2.2 Estonia

Según información del sitio web oficial del gobierno de Estonia (15), este país de cerca de un millón de potenciales electores ha permitido el voto por Internet en 5 ocasiones desde el año 2005 hasta la actualidad (año 2011). En este período, la aceptación y participación ciudadana ha evolucionado desde aproximadamente un 2% de los votantes la primera vez, al casi 25% de marzo de

este año en un incremento, siendo la participación total del 47% de la ciudadanía en 2005 y 63% en 2011. Con anterioridad a la posibilidad de emitir el voto por Internet, los ciudadanos estonios podían entregar el voto de una de las dos formas siguientes: Acudiendo al recinto correspondiente a su propio Distrito Electoral el día designado como "día electoral", o acudiendo a entregar el voto en papel, junto con una acreditación que les identifica, a una "Estación de Votación" abierta a tal efecto días antes de la votación. Esta Estación, se encarga de entregar los votos en el Distrito Electoral del votante. La tercera posibilidad, la de entregar el voto por Internet, está disponible entre el décimo y el cuarto día antes del día electoral. Se mantiene la posibilidad de que entre el sexto y cuarto día antes de la elección, los votantes puedan acudir a la Estación de Votación y entregar el voto en papel, anulando completamente el acto realizado en cualquier momento vía Internet.

2.2.1 *Descripción del Sistema*

Una vez que se han configurado todos los equipos del sistema (Ilustración 1), podríamos distinguir las típicas fases del proceso

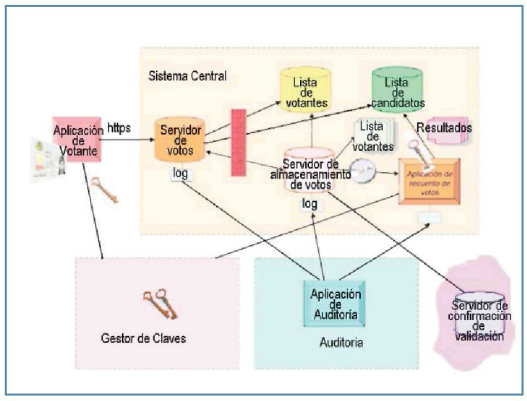

Ilustración 1: Arquitectura global del sistema

de votación: Identificación y autenticación del votante, emisión del voto, recuento de votos y publicación de resultados. El votante instala la *Aplicación de Votante* en el ordenador desde el cual emitirá el voto. Esta aplicación, firmada, permitirá la comunicación con el "Sistema Central" mediante https. En el Sistema Central solo el "Servidor de Votos", está conectado a Internet, el cual está separado por un cortafuego del resto de los elementos del Sistema Central. En la fase de *Identificación y autenticación*, el votante se identifica mediante su Documento de Identidad Electrónico, el Servidor de Votos verifica que este ciudadano figura en la Lista de Votantes, obteniendo además la identificación del Distrito Electoral al que está adscrito, lo que permite al Servidor de Votos obtener la relación de candidatos que envía hacia la Aplicación de Votante para que el votante puede marcar sus preferencias. La seguridad de las comunicaciones es la que ofrece https. En la fase de Emisión de Voto, el votante añade a sus preferencias una secuencia aleatoria (que impide a un atacante establecer una relación uno a uno entre el voto en claro y el voto cifrado) y cifra esta información con la clave pública de la Aplicación de Recuento de Votos, conformando así lo que llama Sobre Interno o también Voto. A este Voto le añade la Identificación y firma del Votante, lo que se asimila a Sobre Externo. Finalmente Sobre Externo es enviado, usando https, hacia el Servidor de Votos. El Servidor de Votos, graba la incidencia en el fichero de *log1* (Ilustración 2) correspondiente a *Votos Recibidos,* y entrega ese Sobre al Servidor de Almacenamiento de Votos, el cual accede al Servidor de Confirmación de Validación para adquirir el Certificado que confirma la validez de la firma digital. En su caso, adjunta el Certificado al voto firmado y envía un mensaje destinado a la Aplicación del Votante, indicando que ha finalizado correctamente el proceso o bien, si el resultado de la comprobación de firma es negativo, anula el voto, grabando la incidencia en el registro *log2* de *Votos Anulados*. A continuación el Servidor de Almacenamiento de Votos comprueba si existe algún voto previamente emitido por el mismo votante, en cuyo caso el voto anterior es sustituido por el nuevo, grabando también la incidencia en el registro log correspondiente a *Votos Anulados.* La fase correspondiente a la *Apertura de la Urna* se realiza una vez finalizada la recepción de votos del día electoral, es decir cuatro días después de finalizar la recepción de votos por Internet. De acuerdo a la legislación, el voto en papel prevalece sobre el voto por Internet emitido por ese votante, con lo cual el sistema electrónico debe recibir la lista de los que han ejercido su derecho en papel y el Servidor de Almacenamiento de Votos procede a descartar los votos de los electores que han votado también en papel, grabando la incidencia en el fichero de log correspondiente a *Votos Anulados*. Finalizado el proceso anterior, ya solo con los

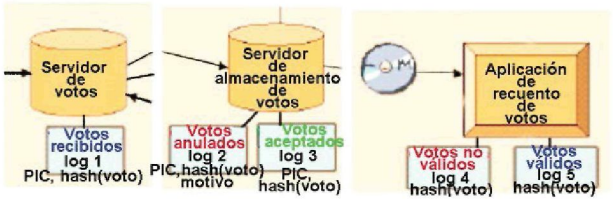

Ilustración 2: Registro para auditoría

votos válidos, se procede a anotarlos en el registro *log3* correspondiente a *Votos Aceptados* y a separar la identificación del votante del voto. Por una parte se configura la lista de los votantes que participaron vía Internet, y por otra, se entrega a la Aplicación de Recuento de Votos todos los votos cifrados, agrupados por Distrito Electoral. Este trasiego de información se realiza mediante un dispositivo extraíble. La Aplicación de Recuento de Votos descifra con su clave privada uno a uno todos los votos, los cuales habrá que relacionar con la lista de candidatos del distrito electoral que le corresponde para proceder al escrutinio, que es finalmente publicado como Resultados. Los votos que contengan una lista de candidatos no adecuada para el Distrito Electoral que les corresponde, son declarados *Votos No Válidos* y anotados en el registro de *log4* correspondiente. Los votos que son contabilizados en el resultado final son anotados en el registro *log5* de *Votos Válidos*. Finalizado el proceso de votación, y las posibles reclamaciones, se destruye la clave privada de la Aplicación de Recuento de Votos.

2.2.2 *Proceso de Auditoría*

Concluido el proceso anterior empieza la labor de la auditoría para el cual se ha ido grabando información en el transcurso del proceso. El Servidor de Votos ha guardado en *log1* el *hash* del voto recibido, esto es, del Sobre interno, junto a un número que identifica al votante (PIC=Personal Identification Code). El Servidor de Almacenamiento Votos habrá recibido, a lo largo de todos los días que el Sistema de Voto por Internet ha estado operativo, la misma cantidad de votos con los votos cuyo *hash* está almacenado en *log1*. El Servidor de Almacenamiento de

Votos ha ido anulando los votos para los cuales el Servidor de Confirmación de Validación no haya reconocido la firma digital del votante y los votos previos de cada votante que ha repetido el voto. Después de cerrar la recepción de votos, este Servidor recibe una lista con la identificación de los votantes que han ejercido su derecho emitiendo el voto en papel, procediéndose a anular los votos por Internet de los ciudadanos que estén en esta lista. En todos los casos se va reflejando en *log2* la identificación del votante, el *hash* del voto y la razón por la que se anula el voto. En *log3* se almacena información correspondiente a todos los votos que se entregarán a la Aplicación de Recuento, de tal forma que *log1=log2+log3*. La lista de los PIC incluidos en el registro de Votos Aceptados (*log3*) debe ser idéntica a la lista definitiva de e-Votantes, cada *hash* de voto debe corresponder con una entrada de voto (Sobre Interno) que se transfiere, agrupado según los Distritos Electorales que le corresponde, a la Aplicación de Recuento de Votos. La Aplicación de Recuento es la que posee la clave que permite descifrar el voto y desligarlo de la secuencia aleatoria. A partir de las marcas del voto, las relaciona con las listas de candidatos del Distrito Electoral correspondiente y guardará registro en *log4* (el *hash* del voto) de aquellos votos que no pueda relacionar con la lista de candidatos considerándolos como *Votos No Válidos* (a diferencia de los que si toman parte en el recuento, cuyo hash se almacena en *log5*). Se debe cumplir que el contenido de *log3* sea igual al de *log4* más el de *log5*.

2.2.3 Valoración

Este sistema funciona bien si es incuestionable la honestidad y la capacitación profesional de las personas responsables de su gestión y operación. El votante hace entrega de un paquete de información, firmado por él y debe confiar en que no será desvelado el contenido de su voto antes de separarlo de su identificación personal. Esta relación de confianza de la ciudadanía hacia la administración existe en otros casos, como es, por ejemplo, el de voto por correo en España. En este último caso, los miembros de la mesa electoral, ciudadanos elegidos al azar entre el cuerpo de votantes e interventores en representación de los candidatos, son los garantes del buen hacer a la hora de abrir los votos. En la información consultada respecto al sistema aplicado en Estonia, no hay mención a la forma en la que se nombran las personas a cargo del funcionamiento del sistema, salvo una rápida referencia a que son distintas personas, las cuales en algún momento podrían actuar en colusión dando origen a la seria amenaza de ruptura del secreto del voto. De acuerdo a la información ofrecida en el sitio web del Gobierno de Estonia, la Auditoría tiene acceso a los registros especialmente preparados para ella. En el caso de que la auditoría acceda solo a los registros *logs*, podría darse el caso de que los resultados publicados guardasen poca relación con la realidad y que los registros *logs* estuvieran maquillados para ofrecer la apariencia de funcionamiento correcto al proceso de auditoría. Si en realidad la auditoría tiene acceso a los registros internos de los sistemas y a la información transferida entre ellos, se puede realizar un control efectivo para verificar que los resultados corresponden a la voluntad de los votantes. Sin embargo, se rompe el secreto del voto puesto que, en última instancia, al verificar que el voto no ha sido anómalamente incluido en el recuento, se debe verificar la validez de la firma que el votante ha puesto en el voto. Por ejemplo, la Auditoría podría repetir el proceso realizado por la Aplicación de Recuento de Votos si recibe el CD con los votos, las Listas de Candidatos de todos los Distritos Electorales y la clave privada que permite descifrar los votos, pero al calcular el *hash* del voto, con la información de *log1* conoce la identificación del votante. A continuación se realiza una descripción de posibles causas de funcionamiento anómalo del sistema.

2.2.3.1 Posibilidad de inserción de votos

Si el Servidor de Almacenamiento de Votos y la Aplicación de Recuento son honestos ningún problema técnico impide el buen funcionamiento del sistema. Solo podría verse afectado el recuento final con los votos insertados por quienes pudieran firmar en nombre de un votante válido, puesto que de lo contrario el voto sería anulado por el proceso al que somete los votos el Servidor de Almacenamiento de Votos. El Servidor de Votos y el Servidor de Almacenamiento de Votos, actuando en colusión podrían añadir votos, incluyendo en el fraude la alteración de los registros *log1*, *log2* y *log3*.

2.2.3.2 Posibilidad de modificación de votos

La firma del votante ofrece garantía de integridad de los datos, por lo que la alteración del contenido del voto sería convertida en eliminación del voto y no en un voto válido para otro candidato. La Aplicación de Recuento trabaja con las Listas de Candidatos de cada Distrito Electoral y con los votos cifrados agrupados por esos distritos que le proporciona el Servidor de Almacenamiento de Votos. Si un voto es cambiado de distrito podría estar dando su apoyo a candidatos distintos de los deseados por el votante. En los registros de *log* no aparece información que ayude a detectar este malfuncionamiento. También es necesario conocer cómo se protegen las Listas de Candidatos frente a manipulaciones, accidentales o fraudulentas, que consigan otorgar los votos a candidatos diferentes de los elegidos por el votante.

2.2.3.3 Posibilidad de eliminación de voto

Esta posibilidad se puede ver desde dos vertientes. Por una parte, el voto es eliminado o destruido para que no tenga apariencia de voto. Lo podría hacer el Servidor de Votos si no es supervisado en su funcionamiento. Incluso podría enviar un mensaje a la Aplicación de Voto para dar a entender al votante que su voto ha sido aceptado. Como la verificación de la firma, que ofrece garantías de integridad de la información firmada, la realiza el Servidor de Almacenamiento de Votos, podría darse el caso de que el voto que recibiera fuese alterado antes de la grabación en el registro *log1* (Identificador del votante junto al *hash* del voto). El *hash* de este voto alterado, junto con el identificador del votante, sería almacenado en *log2* como *Voto Anulado*. Otro fraude que podría cometer el Servidor de Votos sería el descarte del voto, sin guardar registro de él ni menos aún, trasvasado al Servidor de Almacenamiento de Votos, pero enviando mensaje de aceptación a la Aplicación de Voto. La otra vertiente sería la de provocar que el voto no entre correctamente en el recuento final, utilizando los procesos que se realizan en cada sistema. Una de las posibilidades en la que podría incurrir, incluso de forma accidental, se deriva de la actualización dinámica de la Lista de Votantes que se está utilizando en los días que permanece abierta la posibilidad de emitir el voto por Internet. La lista de votantes que ejercen su derecho en papel es otro eslabón débil y debe estar sometida a estrictos a controles de seguridad, de lo contrario se puede convertir en una vía arbitraria de anulación de votos por Internet.

2.2.3.4 Posibilidad de denegación del derecho

Esta posibilidad podría carecer de interés dada la prioridad del voto en papel, pero si llega el momento en que el voto por Internet sea el mayoritariamente aceptado, su buen funcionamiento será

una necesidad. En la actualidad, acaba siendo potestad del Servidor de Votos dar respuesta al votante, y se supone que ha actuado correctamente consultando la lista de votantes de la cual además se obtiene la identificación del Distrito Electoral que está relacionado con los nombres de los candidatos a los que puede votar. Si no se guarda un registro de todos los intentos de identificación infructuosa de votante, se abre la posibilidad de que se niegue arbitrariamente el derecho a voto de legítimos votantes.

2.2.3.5 Posibilidad de ejercer coacción

Una de las principales objeciones que encuentra el voto por Internet es la posibilidad de facilitar la realización de compra y venta masiva de votos. El sistema estonio pone especial énfasis en cuidar el caso de coacción ejercida de forma presencial por parte de una persona que esté vigilando lo que hace un votante. Si el causante de la coacción actúa a título personal, es decir no forma parte de una red más poderosa, la defensa que ofrece este sistema puede dar sus frutos, ya que la víctima puede estar libre para emitir el voto por Internet nuevamente o acudir a depositar el voto en papel. Sin embargo, si la coacción se realiza por parte de una mafia podría tener a su alcance diversos mecanismos. Por ejemplo el de asegurarse de que la víctima no vuelve a tener acceso a la votación, habiendo ejercido la coacción próxima a la hora del cierre, alejando a esta víctima de los recursos que le permitan otra oportunidad. O bien accediendo a la información proporcionada por el registro de Votos Anulados, en cuyo caso podría tomar represalias. Si la víctima sospecha que existe esta posibilidad no se sentirá libre para emitir otro voto. Por otra parte no es necesario disponer de un gran número de personas que ejerzan la coacción si accede al rastro que puede quedar en el ordenador desde el que se vota.

2.2.3.6 Posibilidad de relacionar el voto y votante

Existen varias posibilidades de romper el secreto del voto, ya mencionadas en los apartados anteriores, que se podrían resumir en: la posibilidad de efectuar colusión entre responsables de los sistemas, la posibilidad de ejercer coacción sobre el votante y el ejercicio malintencionado de las tareas de vigilancia mediante auditoría de verificación de funcionamiento correcto del sistema.

2.3 Noruega

El proyecto, que ha sido desarrollado por las empresas SCYTL (16) y ErgoGroup (17), no está sometido a cláusulas de confidencialidad, cumpliendo así las condiciones de la licitación definidas por el gobierno noruego (18). La licitación publicada detalló de forma muy exhaustiva las condiciones que debería cumplir el sistema, tomando importantes y valientes decisiones como fue la condición de que el sistema debería funcionar con software libre, el cual estaba publicando unos meses antes de las elecciones, junto con la documentación del diseño, en los sitios oficiales de la nación. En esta experiencia, que marcará un importante hito en la historia del voto telemático, han participado inicialmente de forma voluntaria los votantes 10 de los 400 municipios, repartidos por la geografía de este país escandinavo (19). Estos municipios son: Bodø, Bremanger, Hammerfest, Mandal, Radøy, Re, Sandnes, Tynset, Vefsn y Ålesund. Aproximadamente el 16% de los cerca de 170 mil ciudadanos con derecho a voto en estos 10 municipios optaron por emitir su voto mediante Internet. La posibilidad de emisión del voto de forma no presencial se habilita en Noruega antes del día designado para entregar personalmente el voto (en papel) en el colegio electoral. El voto electrónico se diferencia del voto anticipado en papel en que el primero se puede emitir múltiples veces, siendo tomado en consideración únicamente el último voto el cual puede ser emitido nuevamente por medios electrónicos, o en papel el día oportuno. Finalizado el proceso las autoridades han puesto a disposición, en sitio web oficial, información sobre el desarrollo de la apertura de votos y posterior recuento. Los resultados de los votos electrónicos se obtienen después de que todas las municipalidades han reportado sus actas, puesto que habrá que retirar del escrutinio aquellos votos que procedan de ciudadanos que han ejercido su derecho a votar en papel, anulando el enviado por vía electrónica. El recuento se realizó delante de público observador, durante la noche electoral en una ceremonia cuyos vídeos están disponibles en el portal oficial del gobierno (20).

2.3.1 Descripción del Sistema

El sistema E-VOTE 2011 (18) consta, por una parte, de una cantidad limitada y reducida de equipos situados en zonas protegidas físicamente y controlados por un grupo restringido de personas designadas para tal efecto y, por otra parte, de los ordenadores ajenos a este control en los que se ejecuta el applet del Cliente de Votación además de los recursos que permiten la autenticación de las personas. Con antelación a la jornada electoral, los ciudadanos que hayan solicitado tener la posibilidad de votar por internet habrán recibido la "tarjeta electoral" que les entrega información importante para enviar el voto e interpretar las respuestas del sistema. También este votante debe disponer de dos dispositivos: uno que le permita comunicarse vía Internet con el equipo que recolecta los votos y otro para recibir vía SMS una respuesta. Se apuesta por diversidad de canales de comunicación como mecanismo que incremente la seguridad del proceso. En E-VOTE 2011 operan de forma coordinada los sistemas de Voto Electrónico, de Administración de Elección y el de recuento de Votos en Papel. Estos sistemas a su vez interactúan, a través de Internet, con grupos de usuarios en los roles de votante, autoridades y operadores de los sistemas. Los eventos críticos que se vayan produciendo en el proceso son almacenados en un "registro inmutable" que basa su propiedad fundamentalmente en la realización de copias del registro cada breve lapso de tiempo. Noruega dispone de un portal que ofrece mecanismos de autenticación electrónica que los ciudadanos utilizan para el acceso a servicios públicos cuando la vía de comunicación es la red Internet. De acuerdo con las condiciones de la licitación, la autenticación de las personas que se relacionan con los dispositivos de votación electrónica (votantes, administradores, operadores, etc.), se realizan utilizando este portal (21).

2.3.1.1 El Dominio de Voto Electrónico

La Ilustración 3 muestra los distintos componentes del Dominio de Voto Electrónico y relaciona los pasos sucesivos por los que pasa un voto desde que es emitido hasta que es tenido en cuenta en el escrutinio. Estos pasos están numerados de forma consecutiva y con línea continua se indica que la comunicación de la información se realiza por medios telemáticos mientras que la línea discontinua, hacia el Dominio Aislado de Voto Electrónico indica que el traspaso de información se realiza por medios manuales. El "Dominio de Servicio de Elección" aparece en este esquema agrupando cuatro grandes bloques funcionales que se encargan de la recolección de los votos, relación con el censo electoral, generación de recibos, almacenamiento y recuento de votos. En el bloque de "recolección de votos" se encuentra la infraestructura que permite realizar las labores de identificación y autenticación de los votantes y, posteriormente, de la recepción y almacenamiento de los votos. El bloque correspondiente a la

"administración del voto electrónico" proporciona la correcta relación con el censo electoral. El bloque de "generación de recibos" se comunica con el bloque de "recolección de votos" mediante una red privada virtual, con extremas medidas de seguridad. Aquí se comprueba la validez de los votos y se genera tanto el recibo como un código de retorno que se entrega al votante por un canal diferente del de emisión del voto: El voto y el recibo se envían por Internet y el código de retorno por el "servicio de mensajes cortos" de telefonía móvil. Como medida de seguridad y garantía de integridad de la información transferida el denominado "Dominio aislado de voto electrónico" recibe por medio de algún dispositivo de almacenamiento masivo portátil (no a través de la red) la información que tendrá que procesar.

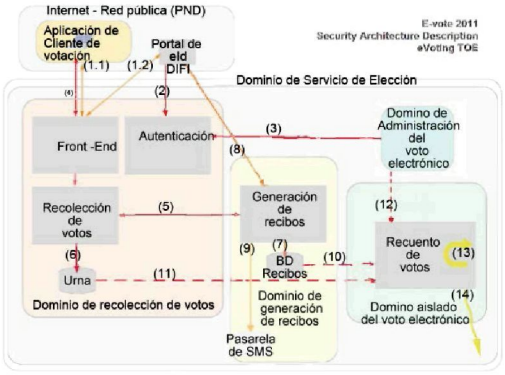

Ilustración 3: El Dominio de Voto Electrónico.

A continuación se describe la sucesión de interacción entre los bloques que aparece numerada de forma consecutiva en la Ilustración 3

1- Por iniciativa del votante, su ordenador se comunica mediante un interfaz Web sobre HTTPS con el Front-End del sistema de votación el cual redirecciona, hacia el portal de identificación oficial de Noruega (22) la comunicación. 2- El servicio de Autenticación establece una sesión en base al "token de autenticación" recibido tras verificar en la información del solicitante la firma digital, el certificado digital, identificador único y sello de tiempo. 3- La Administración de Voto Electrónico verifica la inclusión en el censo y en caso positivo crea una nuevo "credencial de autenticación" que incluye un identificador único, el anterior token, la identificación del votante y la elección en la que puede participar. Esta credencial está firmado digitalmente por el servicio de Autenticación. 4- El servicio de Recolección de Votos recibe del votante el voto cifrado con la clave pública del Comité Electoral (la clave privada se reconstruirá más tarde) y firmado por el votante con los mecanismos digitales proporcionados por el portal de identificación. Pide la aprobación del servicio de Generación de Recibos para continuar su tarea. 5- El servicio de Generación de Recibos obtiene el voto para verificar su validez y generar tanto el Recibo de votación como el Código de Retorno. El primero lo devuelve al servicio de recolección de votos y el segundo lo enviará a la pasarela que lo remitirá al teléfono móvil del votante 6- La Urna (una por distrito) es la base de datos que almacena todos los votos verificados por los servicios de Recolección de Votos y de Generación de Recibos. 7- La base de datos de Recibos almacena todos los recibos que servirán más tarde para validar los votos almacenados. 8- El número de teléfono del votante es suministrado al servicio de Generador de Recibos por el portal de identificación. 9- A través de la pasarela de SMS el votante recibe el código de retorno. Contrastando este código con la información impresa en su tarjeta (de papel) de votación puede verificar que su voto se recibió adecuadamente. 10- Los contenidos de la base de datos de recibos son transferidos de forma manual, mediante el uso un dispositivo de almacenamiento externo, al servidor de recuento de votos. 11- El contenido de la Urna es transferido de forma manual, mediante el uso un dispositivo de almacenamiento externo, al servidor de recuento de votos. 12- El servicio de Administración de Voto Electrónico envía, también mediante dispositivo externo, el censo electoral en el que se distingue los votantes que han solicitado (y recibido) autorización de los que no han iniciado el proceso y entre ellos los que han optado por votar finalmente en papel. 13- El servicio de Recuento de Votos, antes de abrir los votos debe realizar las tareas de depuración del contenido de la Urna, verificando que por cada voto existe un recibo válido, descartando todos los votos cuyos sellos de tiempo sean anteriores al último que proceden del mismo votante, verificando la validez de la firma digital en cada voto y efectuando el proceso de mezcla de los votos de la Urna para evitar que se pueda relacionar el voto con el votante. 14- Los resultados se deben hacer públicos. Otro grupo de interfaces importantes, que no está representado en la figura, es el interfaz con el servicio de registro de eventos y la relación con el módulo Auditor (23).

2.3.2 Valoración

De las condiciones que aparecen en la licitación resulta especialmente importante la condición de publicidad que se le debe dar al funcionamiento del sistema y aplicación de software libre (21). Esta condición parece entrar en contradicción con la obligación de usar el sistema de autenticación MinID (24) que no está sometido a las mismas cláusulas de publicidad. La ciudadanía noruega tiene a su disposición un portal oficial que ofrece mecanismos de identificación electrónica (22) con distintos niveles de seguridad: mediante los servicios ofrecidos por empresa privadas: Commfides (25) y Buypass (26) con el uso de certificado digital y tarjeta inteligente y el requerimiento de identificación presencial de las personas ofrece niveles altos de seguridad, mientras que MinID, de gestión pública no requiere la presencia física de la persona a la que otorga sus credenciales electrónicas protegidas por nombre de usuario y contraseña. Ninguno de ellos hace uso de software libre. En E-Vote 2011 el peso de proteger la identidad del votante recae sobre el propio ciudadano que se ve expuesto a perder mucho más que el ejercicio del voto si cede sus credenciales ya que éstas pueden ser usadas para comprar o vender vivienda, firmar contratos, renunciar a derechos etc. Este método claramente no es aplicable allí donde hay una proporción importante de ciudadanos que no "tienen algo más que perder". Es necesario destacar que con el uso del sistema de autenticación, la firma del voto por parte del ciudadano se realiza con una clave proporcionada por el servicio de autenticación y por lo tanto conocida, al menos, por una entidad distinta a la del propio votante que posee además su nombre y el número del teléfono móvil que recibirá el Código de Retorno. Este cúmulo de información puede anular la eficacia que se argumenta para usar dos canales de comunicación diferenciados para recibir voto y para enviar el código de retorno. Otro factor llamativo de este sistema es que se deberá particularizar el cliente de votación para cada uso puesto que los códigos que genera depende de la cantidad de candidatos y como se organizan políticamente en los partidos. La imposición del uso de un dispositivo telemáticamente aislado donde se realiza el recuento de los votos transferidos por medio de dispositivos de

almacenamiento externos aparece poco fundamentado, dando por supuesto que se puede ejercer mejor vigilancia sobre las personas y dispositivos en los que se realizan las copias que sobre las comunicaciones que puedan realizarse en un entorno de red de área local con los adecuados procedimientos de seguridad en protocolos telemáticos. Como herramienta para contrarrestar las posibilidades de coacción ejercida sobre los votantes, la licitación insiste en permitir la emisión de múltiples votos. Aquí caben las mismas consideraciones aportada al caso estonio. La posibilidad de eliminar los votos emitidos por internet con la emisión del voto presencial en papel el día de la jornada electoral, impide que el recuento electrónico se realice con antelación al voto en papel ya que el servicio de Depuración necesita conocer la lista de ciudadanos que han emitido el voto en papel para retirar el voto en papel cuando sea necesario.

2.3.2.1 Posibilidad de inserción de votos

El servicio de autenticación crea la Credencial de Autenticación, que entre otra información contiene clave privada la que será usada por el votante para firmar el voto. La colusión del servicio de Autenticación con la entidad que genera las tarjetas de votación (u obteniendo los datos de la tarjeta con algún método) permite añadir votos que sería tenidos en cuenta si su sello de tiempo es posterior al voto legítimamente emitido o si el votante decide abstenerse. Debe participar de la colusión también la pasarela SMS para bloquear el envío de mensaje al votante o el servicio de Generación de Recibos para no enviar el número de teléfono del votante (podría enviar número distinto). Ni el servicio de Depuración ni la red de Mezclado podrían detectar este fraude.

2.3.2.2 Posibilidad de modificación de votos

La codificación de las opciones individualizadas para cada votante, el cifrado con la clave pública del Comité Electoral y la firma de la pieza de información ofrece garantías de integridad. Cada voto recibido en el servicio de Generación de Recibos da origen a un SMS hacia el votante. El código de retorno que tiene en su teléfono móvil junto con la información de la tarjeta votación (en papel) permite al votante comprobar que su voto se recibió adecuadamente. Sin embargo si el votante comprueba que su voto ha sido alterado no tiene pruebas robustas para justificar una queja o denuncia. Si comprueba que su voto no ha sido alterado, solo tiene la certeza de que el voto ha sido recibido correctamente y no posee ningún elemento que le permita confiar en el recuento adecuado de los votos. Como se considera válido el último voto emitido, la colusión entre el servicio de Autenticación, que conoce la clave privada con la que el votante firmará el voto, el servicio de Recolección de Votos y, o bien el servicio de Generación de Recibos o la Pasarela SMS, pueden conseguir tergiversar la voluntad del ciudadano. Una vez que el servicio de Depuración ha retirado la firma de los votantes para entregar el contenido de cada urna a la red de Mezclado, podría efectuarse alguna modificación que el votante no detectará.

2.3.2.3 Posibilidad de eliminación de voto

El servicio de Recolección de Votos en colusión con el servicio de Generación de Recibos puede ponerse de acuerdo para eliminar de forma sincronizada ciertos votos junto con sus recibos. Si el servicio de Generación de recibos colude con el sistema que generó los códigos de retorno o posee la misma información tiene el cliente de votación para generarlos, puede realizar una eliminación selectiva de votos.

2.3.2.4 Posibilidad de denegación del derecho

MiniID o el Censo tienen la potestad de autorizar o denegar el derecho a voto, con lo cual son elementos muy críticos en el buen funcionamiento del sistema. El ciudadano que intenta votar por Internet es consciente de esta situación con antelación suficiente como para poder solventar el problema si los procedimientos de reclamación son suficientemente ágiles.

2.3.2.5 Posibilidad de ejercer coacción

La votación por Internet, desde ordenadores no supervisados permite ciertos tipos de coacción tanto evidentes como más elaborados. En el caso de E-Vote 2011, además de las aplicables a cualquier votación por Internet ya comentadas, se añade la posesión por parte del votante de la tarjeta de votación que junto con el Código de Retorno en su teléfono aporta una prueba fiable.

2.3.2.6 Posibilidad de relacionar el voto y votante

El voto está firmado por el votante. Esta situación dura varios días en los cuales se supone que se extrema las precauciones de su custodia. El servicio de Generación de Recibos conoce el contenido del recibo que envía, y sabe a quién se lo envía puesto que ha solicitado a MinID el número de teléfono que debe enviar a la pasarela SMS. El conocimiento de los valores impresos en la tarjeta de votación o la capacidad de cálculo que tiene el cliente de votación, completa la información suficiente para establecer la relación entre el voto y su autor. El Auditor tiene la información correspondiente a todas las entradas y salidas de todos los nodos de la red de Mezclado. Esta es una información privilegiada que le permite romper el anonimato que proporciona la red de Mezclado

2.4 Conclusiones

Es innegable el interés del caso brasileño dado la enorme extensión geográfica que abarca y la gran cantidad de electores que involucra, además de ser pionero en la experiencia. La filosofía que se aplica es la de profundizar en el uso de los avances tecnológicos, manteniendo el principio de recuento granular de los votos en los sitios de votación y transmisión de resultados, enfrentándose al reto de poner las urnas al alcance de los sitios habitados más recónditos. Es necesario perfeccionar este sistema de votación que tiene riesgos inherentes a la tecnología que usa. En el esfuerzo de identificación de estos riesgos, es fácil caer en el error de subestimar el grado en el que pueden atacar también a los sistemas tradicionales. Riesgos que existen tanto en el caso de voto tradicional (voto en papel dentro de una urna) como en voto electrónico son: La posibilidad de coacción que impida a algún votante acercarse al recinto donde debe emitir el voto; la vigilancia física, por medio de cámaras ocultas (incluso portadas por el propio votante), que registren los movimientos del votante; y la colusión de los miembros de la mesa electoral de forma que perjudiquen a alguna opción no representada en ese grupo de personas. Sin embargo, un problema que permanece aún en las zonas oscuras del procedimiento de voto electrónico es la facilidad para relacionar de una forma certera el voto con el votante. La experiencia de votación por Internet de la República de Estonia es muy interesante puesto que se realiza en un ámbito completamente real y vinculante, que está teniendo aceptación nacional a la hora de otorgar validez a los votos emitidos por esta vía. Además cuenta con una amplia aceptación entre los

ciudadanos que, cada vez en mayor número, deciden emitir el voto desde un ordenador situado fuera de los recintos vigilados por las autoridades y otros ciudadanos. Teniendo en consideración la documentación en inglés ofrecida por el gobierno en su sitio web oficial, se aprecian debilidades, siendo la fundamental la que se deriva de la no utilización de mecanismos seguros que garanticen la protección del derecho a voto secreto. El voto que se conserva entre 4 y 10 días almacenado junto con la identificación del votante no está protegido por mecanismos de firma ciega, anonimizadores, ni otros mecanismos equivalentes, sino que se traslada al sistema por Internet las mismas debilidades del voto anticipado en las Estaciones de Votación. Cuando Noruega decide en el año 2008 lanzar el proyecto de voto electrónico, lo hace mediante una licitación en la que participan empresas y consorcios de varias nacionalidades. El proyecto es finalmente adjudicado a las empresas Scytl y ErgoGroup, las cuales desarrollan el proyecto dentro del marco de las condiciones definidas por el estado noruego. Con esto se realiza el diseño, desarrollo y despliegue que permite llevar a cabo, en el primer trimestre de 2011, una experiencia vinculante de voto por Internet, con la participación voluntaria de un máximo de 170 mil votantes. El proyecto E-vote2011 llevado a cabo en Noruega en marzo de 2011 contó con un novedoso despliegue tecnológico e importante esfuerzo informativo lo que lo convertirá, sin lugar a dudas, en una referencia en la historia del "voto por Internet". La licitación marcó con gran nivel de detalle las características que debía tener la implementación. Desde ese punto de vista se cumple la premisa de que el sistema de votación debe satisfacer los requisitos de la sociedad en la que se aplica y no al revés. Las peculiaridades de la sociedad en la que se aplica pueden hacer que el sistema resultante sea poco exportable, aunque siempre hay conclusiones importantes pese a que su validez no sea universal. En gran medida los aspectos críticos que se citan en el apartado 2.3.2 son consecuencia de las especificaciones de la licitación, como por ejemplo todos los aspectos que atañen a la utilización de sistema de autenticación, a la aceptación de múltiples votos de un votante o el empleo de sistema telemáticamente aislado.

3. Bibliografía

1. **Ministério do Planejamento, Orçamento e Gestão.** Instituto Brasileiro de Geografia e Estatística. [En línea] [Citado el:] http://www.ibge.gov.br/home/.

2. **Gobierno de la República de Estonia.** [En línea] http://www.vvk.ee/.

3. **2012 © Statistics Norway.** Statistics Norway. [En línea] http://www.ssb.no/english/.

4. **Tribunal Reggional Eleitoral Rio de Janeiro.** TRERJ - Justificativa Eleitoral. [En línea] http://www.tre-rj.gov.br/site_novo/servicos_eleitor/justificativa/justificativa.jsp.

5. **Gobierno de Brasil.** República Federal de Brasil. [En línea] http://www.brasil.gov.br.

6. **Diebold Election Systems.** [En línea] http://www.diebold.com/.

7. **UNISYS.** [En línea] http://www1.unisys.com:8081/public_sector/clients/featured__case__studies/brazil__federal__electoral__court__.htm.

8. Notable Software, Inc. [En línea] http://www.notablesoftware.com/.

9. Página de Introdução Fórum do Voto Eletrônico. [En línea] http://www.votoseguro.org/.

10. **Tribunal Superior Eleitoral.** Biometria e urna eletrônica . [En línea] http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica.

11. **Ministério da Justiça do Brasil.** Registro de Identidade Civil. [En línea] http://portal.mj.gov.br/ric.

12. **Agência de Notícias da Justiça Eleitoral.** Transmissão de dados via satélite. [En línea] http://agencia.tse.jus.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1343539.

13. **Filho, Amilcar Brunazo.** [En línea] http://www.brunazo.eng.br/voto-e/textos/RelatorioCMind-sumario.pdf.

14. video treinamento de mesarios 2010 parte 1_2.avi . [En línea] http://www.youtube.com/watch?v=1vzWYjOoS-E.

15. **Gobierno de la República de Estonia.** Datos estadísticos. [En línea] 2011. http://www.vvk.ee/index.php?id=12572.

16. **Scytl Secure Electronic Voting, S.A.** http://www.scytl.com. *Secure Electronic Voting. Remote e-voting (Internet voting) and Poll-site e-voting. ::: SCYTL.* [En línea]

17. **EDB ErgoGroup ASA.** http://www.edbergogroup.com/en/ . [En línea]

18. **Ministry of Local Government and Regional Development.** http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/news-about-the-e-vote-2011-project/year/2009/the-final-tender-documentation-for-procu.html?id=598213. [En línea]

19. **Kommunal- og regionaldepartementet.** http://media.regjeringen.no/krd/video/valg2011/Valg_2011_Versjonering_Engelsk.wmv. [En línea]

20. http://media01.smartcom.no/Microsite/dss_01.aspx?

eventid=6316. [En línea]

21. **direktoratet for forvaltning og IKT.** http://www.difi.no/elektronisk-id/about-the-use-of-electronic-id. [En línea]

22. http://www.difi.no/artikkel/2009/11/about-difi. [En línea]

23. **ErgoGroup, Scytl.** *Electronic Voting Software, Electronic Voting Software, EAL 4+.* 2011.

24. http://minid.difi.no/minid/minid.php?lang=en. [En línea]

25. **Commfides Norge AS.** https://www.commfides.com/en/About-Commfides/ . [En línea]

26. **Buypass AS.** http://www.buypass.no/. [En línea]

27. **E-valg_oversikt.** *http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/internettstemmer/E-valg_oversikt_forhandsstemmer_2209_eng.xl.*